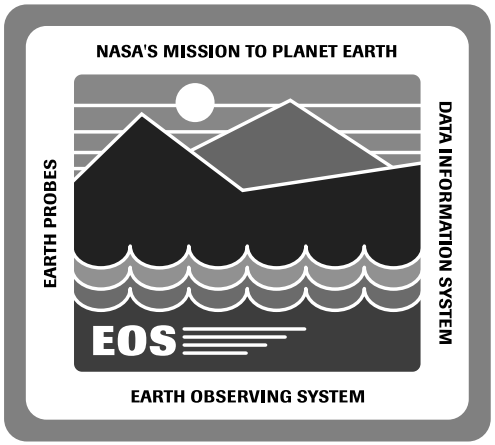
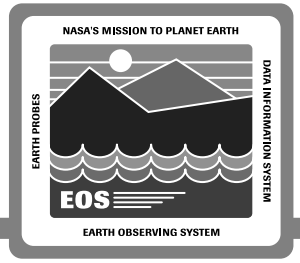


CSMS Security Synopsis

Carl Wheatley

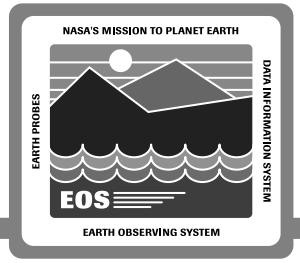
19 January 1995

Synthesis of ISS, CSS, MSS Security Measures



Form of Security	ISS	CSS	MSS
Routing Control			
• Address Filtering	√		√
• Dual Homing	√		
• Firewalls	√		√
Authorization Exchange			
• DCE author./authen.		√	√
• Kerberos authoriz/authen.		√	√
Access Control			
• DCE ACL Managers		√	√
Data Integrity			
• Encrypted Checksums	√	√	
Encryption			
• DCE Encryption		√	
• Kerberos Encryption		√	
Admin Procedures			
• Audit Trails			√
• Logoff/Timeout Features			√
• Preservation of DAAC autonomy		√	√
Physical Measures			
• DAAC & EOC Facility Access	√	√	√
• Separate Bulletin Board Server		√	
• Geographic replication of services/data		√	√
• DAAC isolation LANs	√		
• ECS isolation Cell		√	

Synthesis of ISS, CSS, MSS Security Measures (cont.)

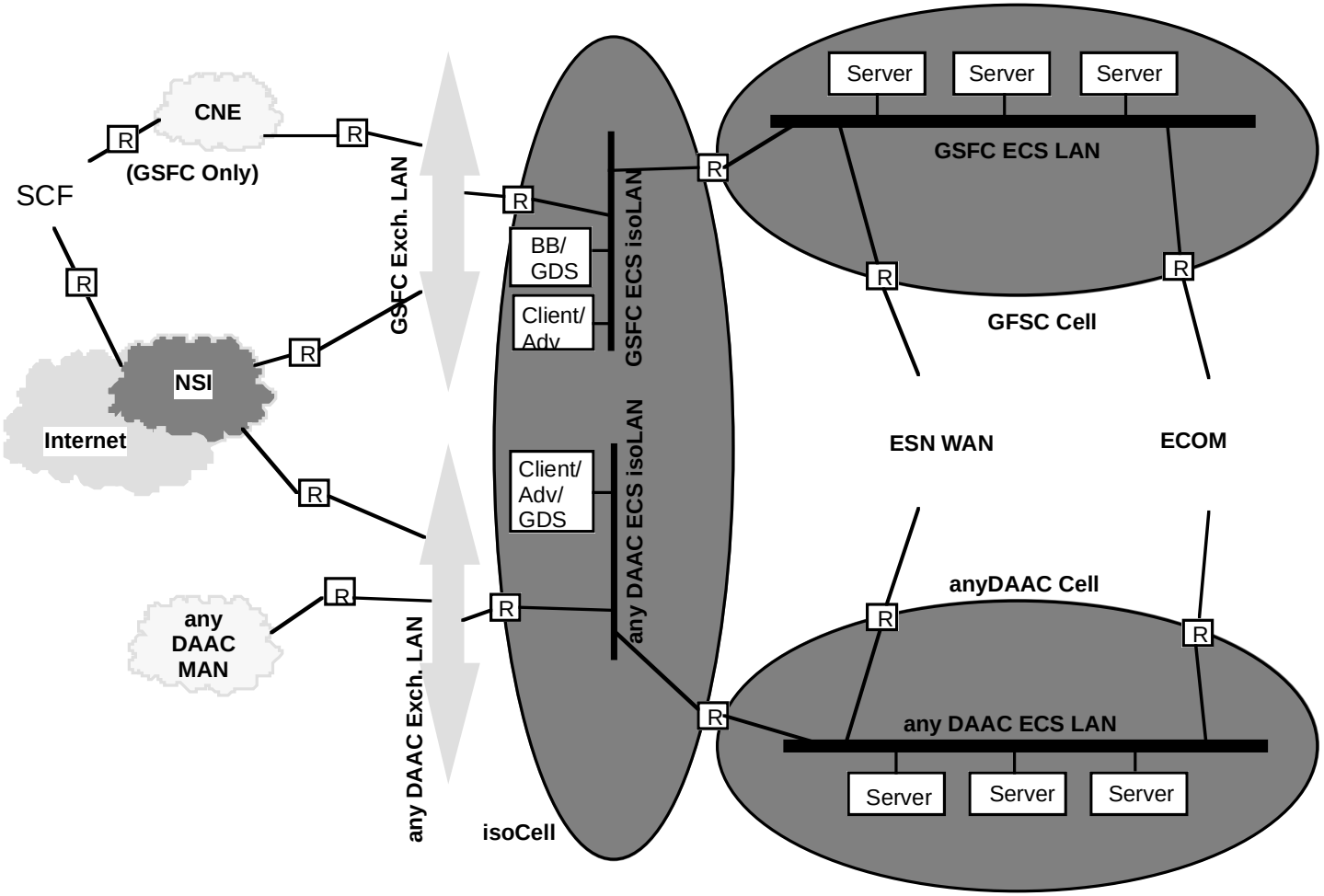


- **CSMS software and hardware design benefits meet or exceed CSMS-relevent C2 requirements per NHB 2410.9A, NASA Automated Information Security Handbook**

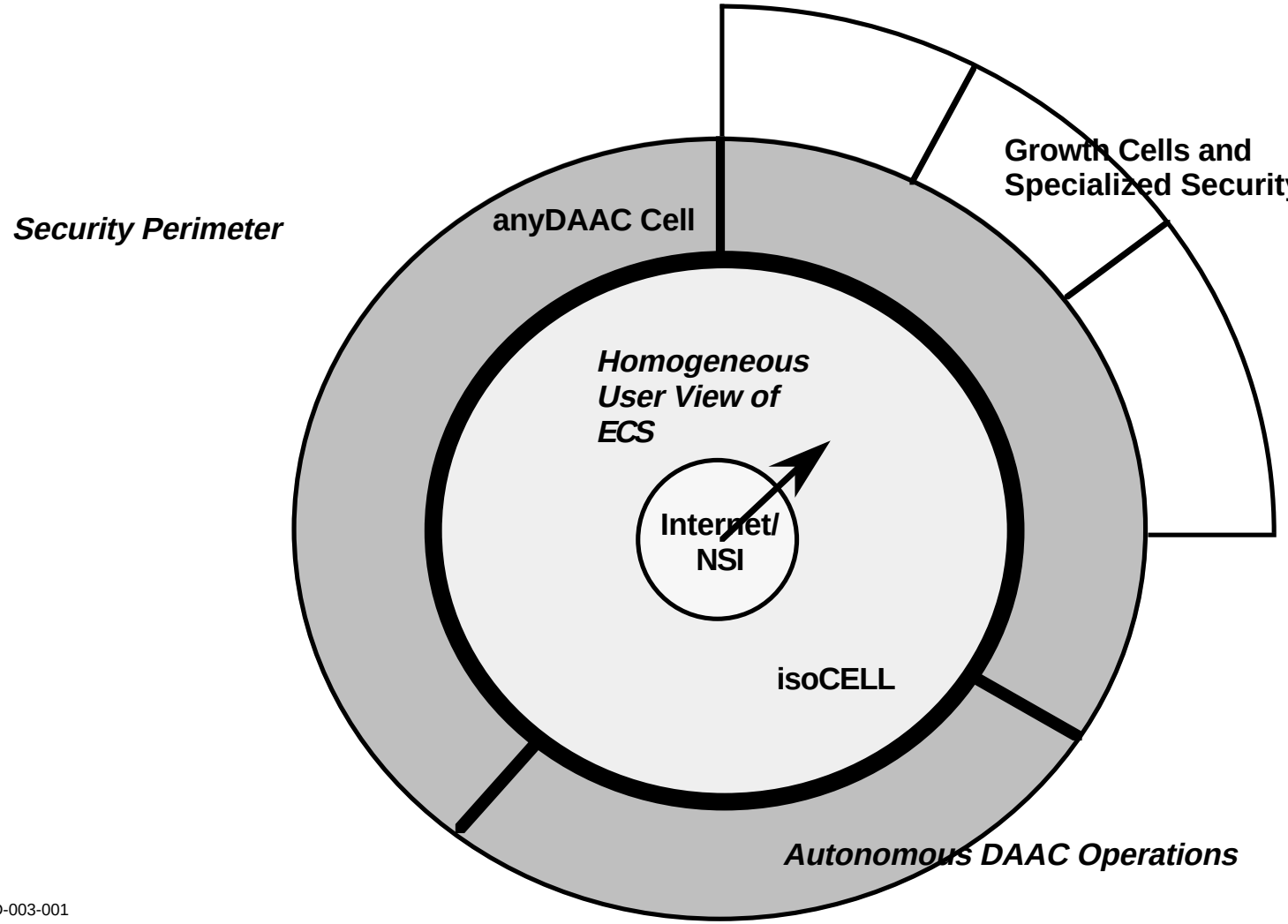
- **Ongoing security risk analysis to be provided PDR + 3 months**

- **Automated security risk analysis software provides detailed risk assessment**

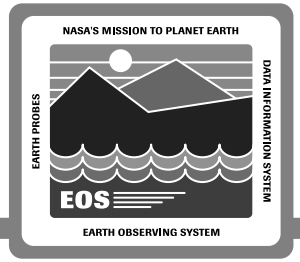
DCE Cell Configuration



DCE Cell Abstraction

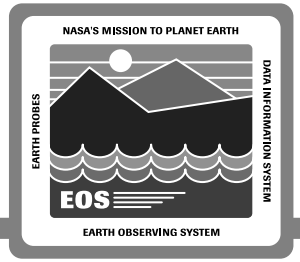


Components of CSMS Security Implementation



Security Need	CSMS Security Implementation	CSS
Authentication	DCE-based Kerberos, Kerberized ftp, Kerberized telnet	X
Authorization and access control	DCE access control; Router-based filters (port/socket at transport layer, and source and/or destination address at network layer); DCE cell configuration / "isolation-cell" partitioning	X
Data integrity	DCE-based RPCs (encrypted checksums)	X
Data confidentiality	DCE-based RPCs (encrypted data) used as required	X
Counter measures for degradation in network or processing resource performance through denial of service attack	Router-based filters	
Security database management	DCE ACL managers, registry database	
Compliance management	MSS COTS & public domain tools for password audits, file system integrity checking	
Intrusion detection	COTS for detecting viruses, worms, Trojan horses, public domain tools (e.g., TCP Wrapper)	
Security reporting	RDBMS	

CSS Security



Based on Kerberos Version 5

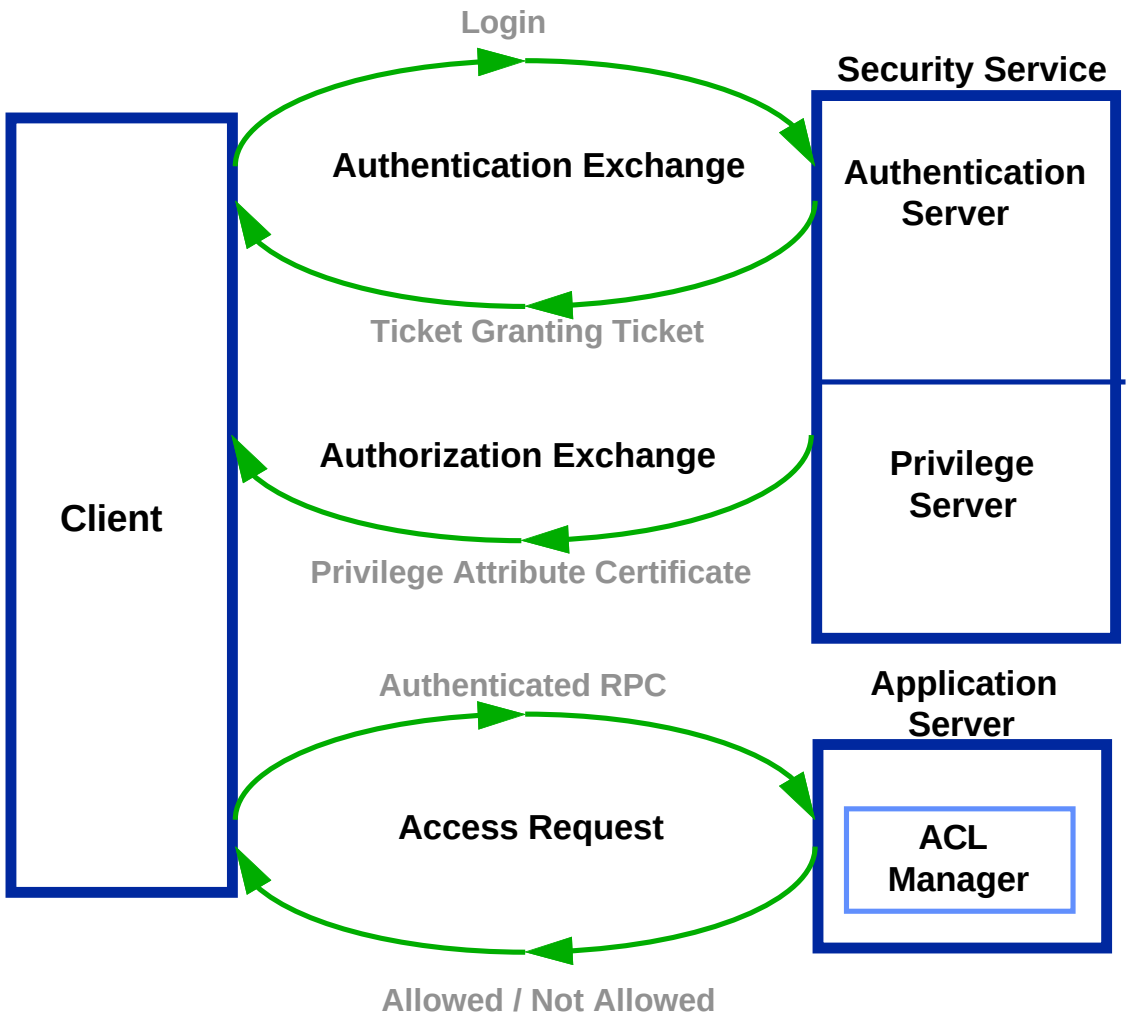
Features

- **Authentication**
- **Authorization**
- **Data Integrity**
- **Data Confidentiality**

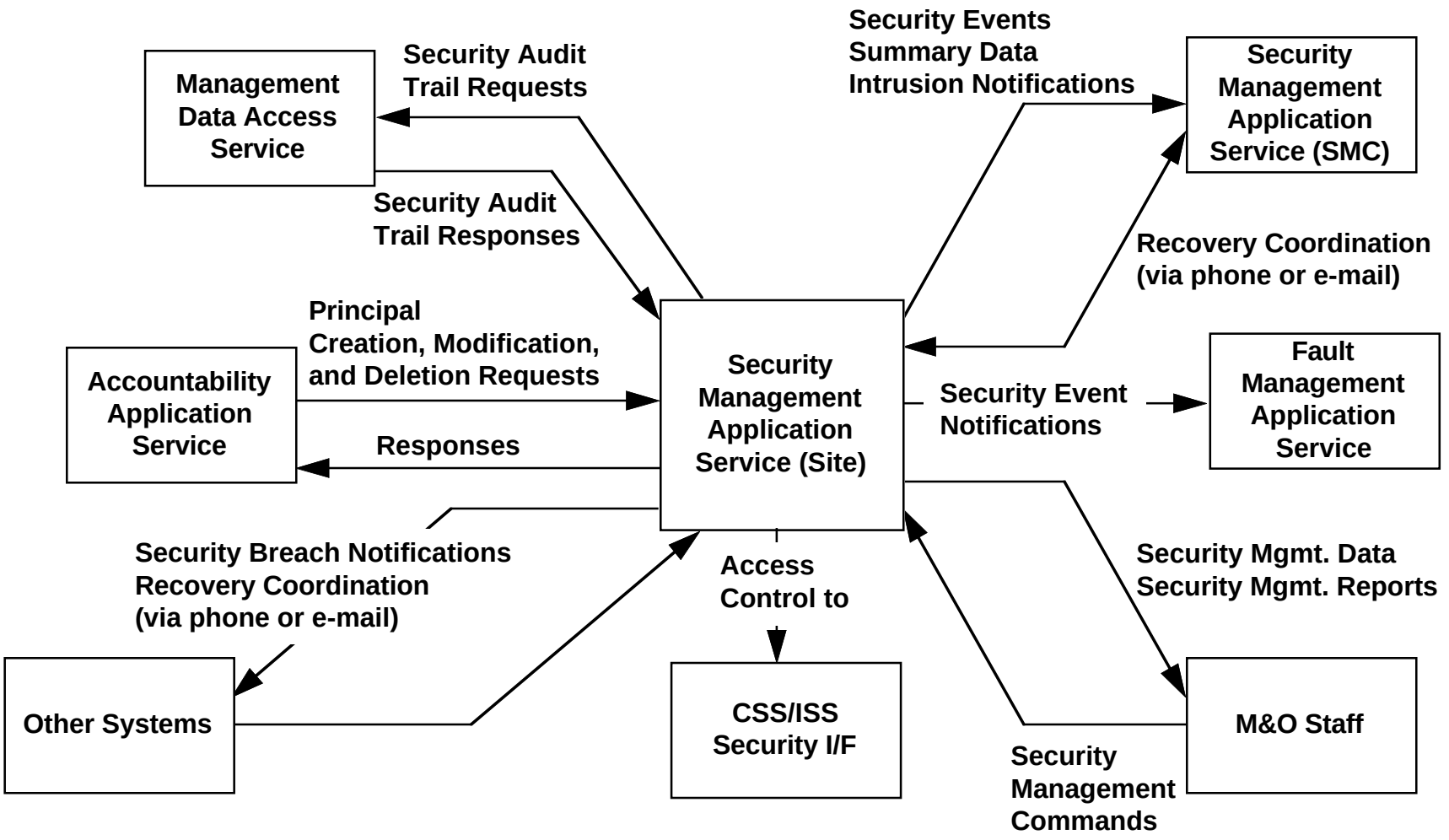
Benefits

- **Fully integrated with DCE**
- **Provides migration to public key**
- **Kerberos developed by MIT**
- **Standards based / COTS based**
- **Compatibility with Public Domain Kerberos**
- **Well tested**
- **No Password in the clear**

Security Concept



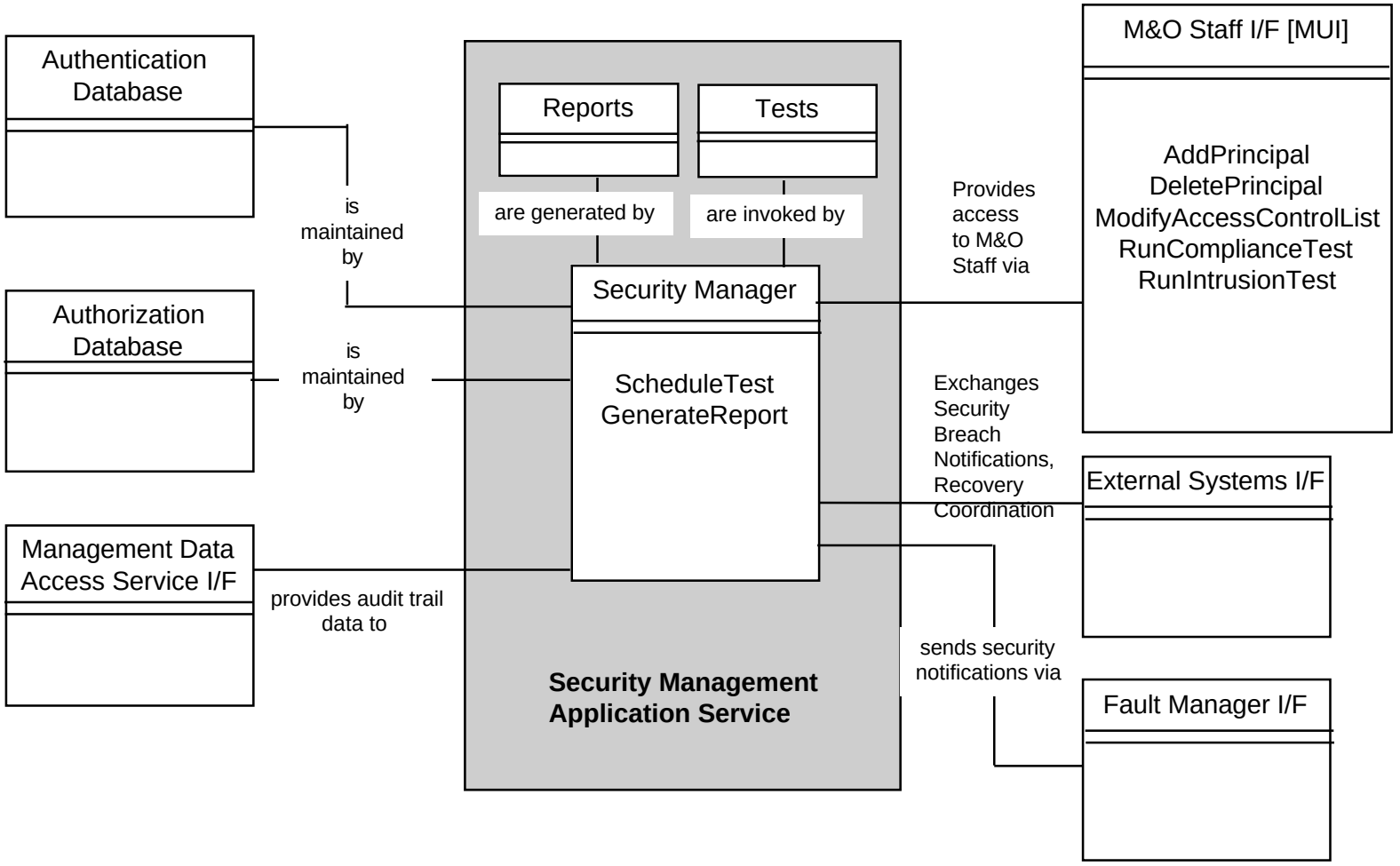
MSS Security Management Context



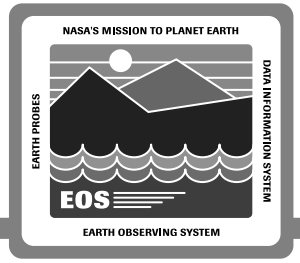
MSS Security Management Capabilities by Release

IR-1 TRMM interface test capabilities	Release A TRMM mission capabilities
Security Database Management **Router-based Address Filtering** **Network-Based Authentication** **Host-Based Authorization**	**Security Database Management** *Router-based Address Filtering* *Network-Based Authentication* *Host-based Authorization* **Network-Based Authorization** **Compliance Management** **Password Auditing** **Privilege Auditing** **File System Integrity Checking** **Intrusion Detection** **Virus Checking** **Unauthorized User Access Detection** **Reporting** **Security Audit Trail Reports** **Compliance Management Reports** **Intrusion Detection Reports**

MSS Security Management Design Decomposition



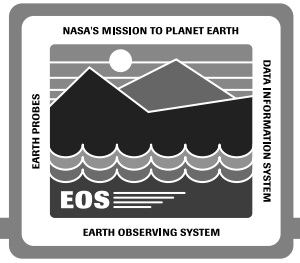
MSS Security Management Scenario



Intrusion Detection:

- **ECS Security policy requires that Compliance Tests be run periodically.**
- **Security Manager allows the periodicity of running the test to be configurable.**
- **A DAAC with no history of breakins decides to schedule these tests weekly. The Security Manager is set up accordingly, accessed via the M&O Staff I/F, to schedule weekly execution of the test.**
- **As a result of a scheduled test, the Security Manager receives a notification that a .rhosts file (a security hole) has been discovered in the home directory of an account.**
- **Security Manager sends a notification of the event via the Fault Manager I/F according to specified criteria maintained by the Security Manager.**
- **M&O Staff, via the M&O Staff I/F, discover that the date of creation of the file is the current date.**
- **(The owner of the account has been on vacation for three days, which indicates that the account has been compromised).**

MSS Security Management Scenario (cont.)

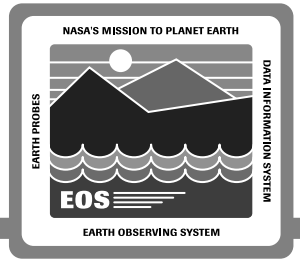


- **Upon initiation by the M&O Staff, via the M&O Staff I/F, security audit data is accessed by Security Manager via Data Management Access I/F to view data records for the activity on the compromised account.**
- **The activity on the account has been only the previous day, with several login failures spaced far apart in time so as not to trip the login failure alert. This indicates that the password has been guessed.**
- **A check on users currently logged on reveals that the compromised account is not currently in use, and the compromised account is disabled.**
- **The M&O Staff notifies the other DAACs, via the External Systems I/F about the incident.**
-

Solution:

The system is taken off-line for further investigation and analysis. Local site policy is modified to run Compliance Tests on a daily basis.

IST Security Requirements



Because ISTs are part of campus/Internet environment, the following security is required:

- **Network security provided via filters on EOC routers**
- **Authentication and Authorization to prevent impersonation of legitimate users**
- **Data Integrity to insure data not modified during transit**

Analysis revealed

- **Software solutions provide better price/performance than hardware (smart card) solutions**
- **DCE effectively provides Authentication, Authorization, and Data Integrity**

IST Security Implementation

Security Need	Implementation
Authentication • Passwords do not appear on net	DCE-based Kerberos encryption
Authorization and Access Control • Integrated with Authentication • Network Layer • Application layer	DCE Access Control Lists (ACLs) and Router Firewalls at EOC
Data Integrity • Encrypted checksums (prevents intentional tampering and unintentional data corruption during transit)	DCE Remote Procedure Call (RPC)